



August 5, 2014

John Morris, Associate Administrator and Director of Internet Policy
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: Privacy RFC2014
Washington, DC 20230

**Re: Common Sense Media Comments on Big Data
and the Consumer Privacy Bill of Rights**

Dear Mr. Morris,

Common Sense Media, a nonpartisan, nonprofit organization dedicated to helping kids and families thrive in a world of media and technology, respectfully submits these comments in response to the National Telecommunications and Information Administration's Request for Public Comment on big data developments and how they impact the Consumer Privacy Bill of Rights.

The evolution of and recent revelations about big data underscore the urgent need to clarify the Consumer Privacy Bill of Rights and enact strong supporting consumer privacy legislation. **Such legislation must recognize that in a big data world, personal information about children, teens, and students is a sensitive data category that presents unique risks and deserves special protections.**

The digital world offers young people limitless opportunities to create, communicate, connect, and learn in new and impactful ways. At the same time, our highly interconnected world aggregates little bits of data into "big data" that may be used by unintended audiences in unexpected ways to deprive individuals of their right to self-determination. We now know that data brokers and other big data players are collecting, mining, and sharing information about virtually every consumer -- *including children and teens*. Data is amassed into extremely detailed profiles, which are used to label and steer individuals. Such ubiquitous data collection and profiling is disconcerting for everyone, but it is particularly troubling for young people, who are growing up, developing, experimenting and learning in a digital world. Big data combine digital footprints into a full body scan, which can then be used to grant or deny admission to future opportunities.

Simply put, big data should not label and limit kids.

Imagine this:

- A student from a less affluent zip code, who can't afford a private tutor, struggles with a math-tutoring app and is labeled as "financially vulnerable."
- A child with an interest in extreme sports (discovered through web browser histories,

YouTube searches, and book purchases) is categorized as a “risk-taker.”

- A teenager, frequently home late (logged by the “smart” home monitoring system), who is friends with a popular crowd on social media and shares posts about parties, is categorized as an alcohol user and “socially influenced” (even if the teen doesn’t drink).

Normal child and teen behavior can categorize, affecting educational options and admissions, employment opportunities, and product offers and pricing.

The Administration’s Consumer Privacy Bill of Rights, released in January 2012, needs to better articulate the vulnerabilities of children, teens, and students in a big data world. The CPBR and codifying legislation should address unique issues presented by their age, level of understanding, and status as a child, teen, or student, to ensure transparency and individual control over their personal information, and to safeguard against the unexpected consequences of big data used beyond the context in which it was collected. We must protect kids and teens from tracking and profiling without their knowledge or consent.

Common Sense Media calls for legislation that builds on the Children’s Online Privacy Protection Act (COPPA) protections for personal information from children under 13,¹ extends protections to teens, and imposes requirements for data brokers.

- Consumer-facing companies, whether online or off, should provide special protections for children and teens:
 - Companies should obtain affirmative express consent from parents (for children under 13) or from teens before collecting minors’ personal information or geolocation.
 - Companies should obtain affirmative express consent from parents (for children under 13) or from teens before targeting them with behavioral advertising.
 - Consumer-facing entities that share personal information about children or teens with third parties, such as data brokers should provide notice to their customers, and should get affirmative express consent from either a parent (for children under 13) or a teen before they collect or share information from or about a child or teen with third parties, such as data brokers.
- Data brokers should provide special protections before profiling children and teens:
 - If a data broker knows or reasonably should know it is collecting information from or about a child under 13, it should stop collecting, until and unless it has affirmative express parental consent.

¹ Under COPPA, online companies that are directed to children under 13 or that know that a user is a child are required to provide notice and obtain parental consent before collecting children’s personal information. 15 U.S.C. § 6502.

- To the extent data brokers collect information from or about children, it should be used only to safeguard the child, such as prevention of fraud and identity theft.
- If a data broker knows or reasonably should know it is collecting information from or about a teen, it should stop collecting, until and unless it has the teen's affirmative express and informed consent.

Children, teens, and students should be able to explore and express themselves freely. They should be given the space to discover and define themselves, before big data does it for them. Failure to safeguard their personal information, coupled with widespread concern about ubiquitous corporate and government surveillance, could jeopardize the collective trust in digital technology. Users may start to self-censor their thoughts, temper their online exploration, and withhold information. This could ultimately chill the right to free expression and squelch opportunities for youth.

Strong safeguards for personal information from and about children and teens would help create a more trusted online environment, where kids can enjoy the benefits of technological innovation without fear of jeopardizing their future. To this end, we need a robust Consumer Privacy Bill of Rights enacted through federal legislation that would extend baseline privacy protections across the commercial sector, from consumer-facing companies to behind-the-scenes data brokers.

Our children can't wait.

I. Big Data Is Tracking Children, Teens, and Students

A. Children, Teens & Students are Providing Increasing Amounts of Data

As explained more fully in Common Sense Media's March 31, 2014 submission to the White House Office of Science and Technology Policy (appended hereto), a number of factors put children, teens, and students uniquely at risk in a big data world.

More data will be collected from today's youth than from any generation ever before. They are the first to have a digital trail spanning the length of their entire lives, if not longer.² They are avid adopters of new technology. And they are particularly heavy users of mobile devices,³

² A quarter of children have an online presence before being born. See, for example, Business Wire Press Release, *Digital Birth: Welcome to the Online World – AVG Study Finds a Quarter of Children Have Online Births Before Their Actual Birth Dates* (Oct. 6, 2010), <http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World>

³ Twice as many young children used mobile in 2013 than just two years prior, and 38% of toddlers under age two have used a mobile device in the last two years. See Common Sense Media, *Zero to Eight: Children's Media Use in America 2013*, 11 (Oct. 28, 2013), available at <https://www.common Sense Media.org/file/zerotoeightfinal2011pdf-0/download>. One in four teens are cell-mostly Internet users, versus the 15% of adults overall, and among teen smartphone owners, that number is one in two. See Pew Research Center & Berkman Center for Internet & Society,

which can collect sensitive data (such as geolocation) anytime and anywhere. In school, the proliferation of educational technology and digitization of school records and activities—from nurse visits to student keystrokes—means digital dossiers that are lengthier and stickier than any paper file.

Young people seem wired to share more information. Children may not appreciate the sensitivity of what they are sharing. And teens live in a culture that promotes sharing,⁴ with no signs of abatement (a recent research study found that teenage use of Facebook increased in the last two years).⁵ Teens also tend to act impulsively without fully thinking through the consequences.⁶ Young people often do not understand what data they are sharing and with whom it will be shared afterwards.⁷

Moreover, as also detailed in Common Sense Media’s March 2014 Comments (Appendix A), young people are being monitored not only in their free time, but also in school and while completing their homework. Schools and teachers are experimenting with educational learning platforms, fingerprint-purchased meals, and digitized student records in the cloud. Educational technology (“ed tech”), used wisely, has the potential to positively transform America’s schools, enhancing student learning and improving school efficiency. At the same time, it also brings a host of privacy concerns. As the White House Big Data Report recognizes, student data can be very personal.⁸ Student data can reveal academic progress, health information, disciplinary records, and even eligibility for free or reduced price meals. Thus, “[t]he big data revolution in education ... raises serious questions about how best to protect student privacy as technology reaches further into the classroom.”⁹

Many educators and educational institutions have not been trained to contend with today’s rapidly advancing technology. Teachers may be enticed by “free” apps that turn out to be paid for with students’ data. For their part, ed tech vendors have a mixed record of protecting student data. Many indicate a desire to do the right thing, but many also have opaque privacy policies and unclear sharing practices.¹⁰

Teens and Technology 2013 (Mar. 13, 2013), available at http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_TeensandTechnology2013.pdf.

⁴ 90% of teens have used social media. See Common Sense Media, *Social Media, Social Life: How Teens View Their Digital Lives*, 9 (June 26, 2012), available at <https://www.common Sense Media.org/file/socialmediasociallife-final-061812pdf-0/download>.

⁵ Reed Albergotti, *Survey: Teens Say They Are Using Facebook More*, Wall St. J. Digits Blog (June 24, 2014, 6:00 AM), <http://blogs.wsj.com/digits/2014/06/24/survey-teens-say-they-are-using-facebook-more/>.

⁶ FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, 70 (Mar. 2012); see also *infra* p. 9-10 and note 30.

⁷ Pew Research Center & Berkman Center for Internet & Society, *Teens, Social Media, and Privacy*, 2 (May 21, 2013), available at http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

⁸ Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (May 2014) (“White House 2014 Big Data Report”).

⁹ *Id.*, at 25.

¹⁰ Benjamin Herold, *Ed-Tech Vendors’ Privacy Policies Under Scrutiny*, Education Week (Apr. 16, 2014)

B. Data Brokers Are Collecting Information About Young People, Online and Offline

With the exponential proliferation of digital data about kids, the recent FTC Data Broker Report has substantiated one of the most significant risks for young people: that big data is collecting, storing, mining, and sharing information about children and teens.¹¹ The FTC Report confirmed that some data brokers include information about children and teens in products they sell to their clients.¹² Others “suppress” the information related to children and teens and do not include it in their products—but apparently make no effort to stop collecting, storing, and perhaps even mining, such data. And some data brokers simply rely on their sources to “suppress” information about children and teens, turning a blind-eye to whether or not they are collecting such information or including it in their products.

Importantly, “suppression” does not mean deletion. Neither data brokers nor their sources have said what they do with the data when a teen turns 18. But it seems likely that they start using it then (if they haven’t already). Otherwise, why keep it at all?

One rationale given for collecting or providing information about children and teens is to prevent fraud. This in itself cannot justify unlimited collection or use of children and teen personal data. Indeed, data brokers acknowledge this implicitly in instances when they “suppress,” or rely on their sources to “suppress,” such information for a minor.

Data brokers’ sources are myriad and opaque. It is doubtful that all sources are “suppressing” information related to children and teens, especially given the vast number of third-party trackers that are explicitly targeting children for advertising and profiling. For instance, in May of 2014, TRUSTe found 1,110 third-party trackers, including 644 unique tracking organizations, on the top 40 websites used by kids.¹³ TRUSTe found an average of two-dozen trackers on preschool and education sites, and even more on kids’ entertainment and gaming sites.

Recent reports have explained how data brokers combine data from hundreds or thousands of data points, creating an incredibly detailed profile. Even the most innocuous seeming data can end up contributing to a rich and potentially incriminating individual profile. As the White House Report explains, “integrating diverse data can lead to what some analysts call the ‘mosaic effect,’ whereby personally identifiable information can be derived or inferred from datasets that do not even include personal identifiers, bringing into focus a picture of who an individual is and what he or she likes.”¹⁴

¹¹ FTC, *Data Brokers: A Call for Transparency and Accountability*, 21 (May 2014).

¹² The only stated purpose of such inclusion was for fraud prevention. *Id.*

¹³ Press Release, TRUSTe, New Study Finds 644 Unique Third Party Trackers (Jun. 19, 2014), <http://www.truste.com/about-TRUSTe/press-room/news-study-finds-644-unique-third-party-trackers>.

It is unclear if these trackers provide their information to ad networks, data brokers, or both; regardless, they are all part of a sharing ecosystem. See, for example, Display Advertising Technology Landscape, LUMA Partners LLC (Dec. 31, 2010), http://cdn.theatlantic.com/static/mt/assets/science/display_advertising_ecosystem_011011-1024x741.png.

¹⁴ White House Big Data Report, *supra* note 8, at 8.

This picture becomes even more focused when data brokers combine online data with offline data, a practice known as “onboarding.”¹⁵ Marketers admit to using “onboarding” to target consumers online based on their offline behavior. And they appear to be doing the reverse as well—targeting people offline based on browsing patterns online.¹⁶ We can expect more of such data merging and marketing across online and offline platforms in the future.¹⁷

Offline data is expected to expand exponentially with the growth of wearables, facial recognition technology, and the internet of things. As offline data collection moves from the credit-card reader to the street camera or the smartwatch, more offline data will be collected from children and teens. This trove of offline data will be combined with ever-more online data¹⁸ into even more detailed and potentially intrusive personal profiles at even younger ages.

The personal and sensitive data collected about young people may include everything from social media posts (anonymous or not) to geolocation, the content of emails and texts, the hours spent on various devices, online videos, newspapers, and books, school research interests, educational app progress, metadata, in-school grades, nurse visits, food choices, health and biometric information, in-store and online purchases, friends and family, and economic background.

Given the exponentially increasing amount of data created, collected, and combined, online and offline, coupled with the dwindling amounts it costs to store and mine such data, there are few practical constraints on big data brokers. Thus, legal, ethical and other constraints are needed to ensure that young people can grow up free of constant surveillance, free of digital labeling and related limitations.

C. Big Data Is Labeling and Limiting Minors in Ways That Will Have Long-Term and Little-Understood Consequences

Big data has the power to determine and decide. Recent scholarship demonstrates the extent to which individuals are being scored and categorized.¹⁹ They are labeled as everything from

¹⁵ FTC Data Broker Report, *supra* note 11, at 29.

¹⁶ *Ibid.*

¹⁷ See, e.g., Kate Kaye, *Acxiom Acquires LiveRamp to Boost Offline-to-Online Data Capability*, Advertising Age (May 14, 2014), available at <http://adage.com/article/datadriven-marketing/acxiom-buys-liveramp-offline-online-data-capability/293212/>.

¹⁸ Ninety-percent of data was created in the last two years. See Edith Ramirez, Chairwoman, FTC, Speech at the Media Institute: Protecting Consumer Privacy in a Big Data Age (May 8, 2014).

¹⁹ E.g., Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); Pam Dixon & Robert Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* (Apr. 2, 2014), available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf;

Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations Majority Staff, *A Review of the Data Broker Industry* (Dec. 18, 2013), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577; FTC Data Broker Report, *supra* note 11

allergy sufferers to sports enthusiasts to unlikely to pay the bills.²⁰ This ranking is not limited to adults. First-graders may be labeled as drop-out risks, and elementary students are being counseled on certain careers.²¹

Labeling and predictions of future behavior can occur not just on the basis of past behavior, but on the basis of algorithmic inferences. FTC Chairwoman Edith Ramirez has explained that big data can label people “not because of what they’ve done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in certain ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions.” She terms this “data determinism,” and has expressed concerns about “discrimination by algorithm” and “arbitrariness-by-algorithm.”²²

Other scholars have argued that algorithms are worse than arbitrary -- they are *biased*. This is because “human beings program predictive algorithms,” so “their biases and values are embedded into the software’s instructions.”²³

Arbitrary and biased labeling can be extremely limiting. Predictive algorithms may show only news articles from a certain point of view. Search results may provide medical information based on a computer’s assessment of likely ability to afford treatment. College pamphlets or career guides might make their way into some postal and e-mail boxes, but not others. What’s more, big data and scoring systems “have the potential to take a life of their own, contributing to or creating the situation they claim merely to predict.”²⁴

Big data knows more and more about us with each passing day, and can channel our choices, our decisions, and even our emotions, without our knowledge. For example, earlier this year we learned that in January 2012, Facebook had intentionally altered news feeds of hundreds of thousands of its users (including teens) to make them happy or sad. Who is to know what other secret experiments Facebook, or a data broker the public has never heard of, has conducted on users?

Data collectors have the power to steer people’s lives and drive individual decisions of in ways that are opaque and not understood. Big data combine digital footprints into a full body scan. Big data’s most pronounced effect surely will involve kids and teens. Data may be collected during every moment of their lives, including key formative years during their childhood and adolescence, when exploration is encouraged and desirable. Data will also be

²⁰ Dixon, Gellman, *supra* note 19, at 8; FTC Data Broker Report, *supra* note 11, at 21.

²¹ Sarah Sparks, *Data System Flags Dropout Risks by 1st Grade*, Education Week (August 6, 2013), available at <http://www.edweek.org/ew/articles/2013/08/07/37firstgrade-2.h32.html>; Stephanie Simon, *Big Brother, Meet the Parents*, Politico (June 5, 2014), available at <http://www.politico.com/story/2014/06/internet-data-mining-children-107461.html>

²² Edith Ramirez, Chairwoman, FTC, Keynote Address at the Technology Policy Institute Aspen Forum: Privacy Challenges in the Era of Big Data: A View from the Lifeguard’s Chair (Aug. 19, 2013); Edith Ramirez, *supra* note 18.

²³ Citron, Pasquale, *supra* note 19, at 4.

²⁴ *Ibid*, at 33.

collected as they research and develop in school. As students learn, big data will be learning about them. While this can have positive benefits in the individualized education context, it is difficult to ignore the risks. This data could be viewed by unintended audiences and may result in unexpected consequences.

Imagine if a grade school student struggles with a math app. She is also clocked at turning in every test at the very end of class, always taking the full time. She is labeled as a slow learner, and put in remedial classes the next year. The school's "career counselors" come to remedial classes to talk about trade schools, not college. The ads she sees online, and the informational materials she receives in her email box and at her house all trumpet the same message. She does not go to college. She does not end up in a high-paying job.²⁵

Young people, whether in school or out of it, need to be able to safely explore and express themselves without fear of being labeled or pigeonholed by invisible, automated decisionmakers. They need the freedom to make mistakes, try new things, and find their voices, unencumbered by the looming threat of a permanent digital record.

II. A Robust Consumer Privacy Bill of Rights and Strong Codifying Legislation Is Needed Now

In order to reap the benefits of big data while also responding to its risks, we must adopt a legal framework that reflects the unique sensitivity of child, teen, and student data and creates a trusted environment for today's youth, with transparency and individual control over commercial tracking, targeting and profiling. There is deep public concern about this issue. Eighty-seven percent of consumers with a child in the household avoid doing business with companies they do not believe protect their privacy.²⁶ Eighty-nine percent of Americans believe it is extremely or very important to keep personal information about their kids private from corporate tracking.²⁷

A. The CPBR Should Provide Meaningful Transparency and Control for Young People and Limit the Unintended Consequences of Data

The Consumer Privacy Bill of Rights rightly recognizes the unique characteristics of kids and teens may require greater protection for their privacy interests and personal data than for adults. The CPBR's "Respect for Context" principle states that, "Consumers have a right to expect that

²⁵ Citron and Pasquale describe another frightening scenario involving a recent college graduate: she can't get a job after graduation, gets a low "employability" score on this basis, finds only part-time work which reduces her credit score, and then suffers more because of her low credit score, never finding a full-time job. Citron, Pasquale, *supra* note 19, at 32.

²⁶ 2014 TrustE Kids Privacy Index, *supra* note 13. This is particularly problematic because not a lot of consumers do believe companies protect their privacy. A recent Gallup poll found that only 1 in 5 consumers has a lot of trust that businesses will protect their privacy. See John Fleming & Elizabeth Kampf, *Few Consumers Trust Companies to Keep Online Info Safe* (June 6, 2014), <http://www.gallup.com/poll/171029/few-consumers-trust-companies-keep-online-info-safe.aspx>.

²⁷ Memorandum from Anzalone Liszt Grove Research, Americans Concerned about Privacy from Corporate and Government Surveillance (Mar. 31, 2014), *available at* http://media.wix.com/ugd/c4876a_e8f4ee3b207344d9aac9a3403118ca9c.pdf.

companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.” As the White House 2012 report elaborated: “[T]he age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers.”²⁸ Further, the report stated that the CPBR principles “may require greater protections” for child and teen data.²⁹

According to the CPBR, if companies use or disclose personal data for purposes that are not consistent with the context in which consumers originally disclosed the data, they should provide heightened Transparency and Individual Choice. This should apply, for example, if consumer-facing online companies share consumers’ personal information with behind-the-scenes data brokers.³⁰ When children’s or teens’ personal data is involved, this should be considered sensitive information that requires affirmative opt-in consent before it is used to target ads and before it is shared with third-party data brokers for profiling and other purposes.

Companies should consider greater protections for child, teen, and student data when considering other fair information practice principles. Age, level of understanding, and student status affect multiple principles in the CPBR. They affect what constitutes an appropriate level of transparency and notice, which in turn enables choice and individual control. They also affect what constitutes appropriate collection, retention, use, and data security.

- Young children under 13 generally lack the ability to provide consent. The Children’s Online Privacy Protection Act (COPPA) requires sites, services, and apps that are directed to children under 13 or that have actual knowledge that a user is under 13 to provide notice to parents and obtain express verifiable parental consent before collecting personal information. Transparency and notice should thus enable parents to make choices. If a parent can’t consent, there should be limited or no collection. Children’s data should be kept securely, used in age appropriate ways, and maintained only for a limited time.
 - The White House 2012 Report describing the CPBR adds that children may be particularly susceptible to privacy harms, and that the “Administration looks forward to exploring with stakeholders whether more stringent applications of the CPBR – such as an agreement not to create individual profiles about children, even if online services obtain the necessary consent to collect personal data – are appropriate to protect children’s privacy.”³¹

²⁸ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 15 (Feb. 2012).

²⁹ *Ibid.*

³⁰ See White House 2012 Report, *supra* note 28, at 15; FTC Data Broker Report, *supra* note 11, at 52 (proposing that legislation require consumer-facing sources (1) to provide a prominent notice to consumers that they share information with data brokers and give consumers the ability to opt out; (2) to obtain consumers’ affirmative express consent before collecting and sharing sensitive information, such as certain health information, with data brokers; and (3) provide the names of the data brokers and information/links to opt-out rights offered by these data brokers).

³¹ White House 2012 Report, *supra* note 28, at 17-18.

- Teens typically need more information in order to meaningfully consent and exercise informed control. Teens are in a unique developmental state. Studies have demonstrated that the “reward regions” in teen brains are hyper-excitabile.³² Their limbic system, which is responsive to rewards, develops faster than their pre-frontal cortex, which governs impulse-control.³³ Teens are apt to respond quickly to rewards without fully considering risks.³⁴ They could give over information in haste without understanding the costs. Companies should respect teens’ unique state in providing notice and obtaining consent. By providing teens with the ability to opt-in, companies can allow teens to pause, consider consequences, and get more information. As the FTC has explained, setting more privacy-protections by default “can function as an effective ‘speed bump’ for this audience and, at the same time, provide an opportunity to better educate teens about the consequences of sharing personal information.”³⁵ Moreover, teens may better approximate the true value of their data when they feel they have ownership of it to begin with.³⁶ When teens do consent to share their data, they should be able to trust that companies will keep it securely and not for longer than is necessary.

Student data is often collected without much notice or choice to educators, parents or students. Given this context, ed tech providers should provide extra transparency, so schools, parents and students can make informed choices about which ed tech vendors to use. Further, there should be particular attention to context and focused use in such circumstances. Students and families have a right to expect that when personal data is collected from or about K-12 students in school or in connection with school activities, it will be maintained securely, and used and disclosed only to fulfill the educational purpose for which it was collected.

We need strong legislation codifying the CPBR principles set forth above, to require transparency and individual control, and protect against unforeseen consequences when minors’ sensitive information is used out of context.

³² Adriana Galván et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents*, *Journal of Neuroscience*, June 21, 2006; Adriana Galván and Kristine M. McGlennen, *Enhanced striatal sensitivity to aversive reinforcement in adolescents versus adults*, *Journal of Cognitive Neuroscience* (2013).

³³ *Id.* and B.J. Casey et al, *The Adolescent Brain*, *Developmental Review* (Feb. 11, 2008).

³⁴ Galván et al., *supra* note 32, at 284-296.

³⁵ FTC 2012 Privacy Report, *supra* note 6, at 60.

³⁶ In a study conducted by Alessandro Acquisti, shoppers were less likely to exchange their information for only a few dollars if they felt that the information was theirs at the start (see Somini Sengupta, *Letting Down Our Guard with Web Privacy*, *N.Y. Times* (Mar. 30, 2013).) One group of shoppers was offered \$10 gift cards, with an extra \$2 offered in exchange for shopping information. Half rejected the offer. A second group was offered \$12 gift cards, with the choice to take \$10 if they didn’t want to share their shopping data. Only ten percent asked that their data be private.

B. Baseline Privacy Legislation Should Provide Extra Safeguards for Children's and Teen's Personal Information

There is bipartisan agreement that children should not be tracked without their parents' consent or even their knowledge, and growing bipartisan support for the notion that teens deserve similar protections. And there is bipartisan agreement that student data should be used to improve education, not to sell products or amass profiles. Children's, teens', and students' personal information has appropriately been recognized as sensitive and deserving of extra protections.³⁷

1. Privacy Legislation Should Require Companies to Provide Special Protections for Children and Teens

The online and offline worlds are blurring, and kids deserve to have their personal information protected however it is collected. Teens also deserve to have more notice, choice, and control over the collection of their data, appropriate to their age and level of understanding. Therefore, Common Sense Media has supported certain high level principles for teens:

- 1) Teens and parents (for children under 13) should have to “opt in” and provide affirmative express consent before their personal information or geolocation information is collected.
- 2) Teens and parents (for children under 13) should have to “opt in” and provide affirmative express consent before behavioral advertising is targeted at them or before third-party profiles are created about them.
- 3) Companies should establish policies for transparency, collection, use, disclosure, retention, and security of minors' personal information based on the fair information practice principles.

Many of these principles are found in the bipartisan, bicameral Do Not Track Kids Act of 2013, which would provide important baseline protections for young teens as well as enhance COPPA protections for children under 13. The bill would require that websites and services directed at teens ages 13 to 15, or who know they are collecting personal information from kids aged 13 to 15, gain consent before collecting personal information (including geolocation). The bill would also allow children and teens to remove personal information via an “eraser button”.³⁸

These principles should be incorporated in the Administration's baseline privacy legislation. Public support for such legislation is high. In addition to the almost nine out of ten Americans

³⁷ White House 2012 Report, *supra* note 28, at 15; FTC 2012 Privacy Report, *supra* note 6, at 59-60. White House Big Data Report, *supra* note 8, at 25.

³⁸ Common Sense Media was pleased to support the passage of California's SB 568, Privacy Rights for California Minors, which provides an eraser button for minors to remove their own postings on social media and other sites.

who believe corporations shouldn't track kids, almost eight out of ten believe that companies should get permission from teens aged 13 to 15 before collecting personal information about them or sending them targeted advertisements.³⁹

2. Privacy Legislation Should Require Data Brokers To Limit Collection from and about Children and Teens

The Administration's privacy legislation should also close the data broker loopholes and ensure that they too respect sensitive youth data.

The FTC Data Broker Report confirmed that data brokers are collecting information about minors. The one plausible explanation for such collection is to prevent fraud.

The use of a child's or teen's data for fraud prevention purposes is one thing. But in order to flag a purchase for fraud, all that is necessary to know is the age associated with the device or ID making the transaction. It is not necessary to know that the device is also partial to cowboy cartoons, that the device has recently asked puberty-related questions on a health site, or that the device's progress in a book is well-behind grade-level expectations and indicates a likelihood of a learning disability. Nonetheless, this information may be collected.⁴⁰ And if it happens to be "suppressed," there is no telling what happens when the child turns 18. It is entirely conceivable that, just as teens are coming of credit-card age, a detailed profile, amassed about them since birth (or before), will be used to tailor not only ads, but also to determine news, housing, health, and education information, channeling them into one offer or opportunity or another, possibly with life-changing ramifications.

Legislation should require data brokers to refrain from collecting personal information from or about children and teens without express, informed consent. The principles underlying COPPA, which requires parental consent before online collection of personal information from children under 13, should apply equally to information collected offline from children and information collected and compiled by data brokers from or about children.⁴¹ Teens, likewise, deserve the opportunity to opt-in to data brokers collecting, compiling, and profiling their personal information.

Personal information about children and teens is sensitive, whether collected online or offline, directly or indirectly, and ought not be collected, compiled, profiled or shared by data brokers without the informed, affirmative express consent of the child's parents or the teen.

Accordingly, Common Sense Media proposes that the Administration's privacy legislation incorporate the following principles:

³⁹ Anzalone Liszt Grove, *supra* note 27.

⁴⁰ If onboarding is occurring, the device profile might also include information about local ice cream store preferences, or matinee movie visits.

⁴¹ *Cf.* FTC Data Broker Report, *supra* note 11, at 55.

- 1) Consumer-facing entities that share child or teen data with third parties such as data brokers should provide notice to their customers, and should get affirmative, express opt-in consent from either a parent (for children under 13) or a teen before they collect or share information from or about a child or teen.⁴²
- 2) If a data broker knows or reasonably should know it is collecting information from a child under 13, it should stop collecting, until and unless it has affirmative, express parental consent. This is consistent with COPPA's framework, and would prevent any backdoor methods of collecting personal information, including persistent identifiers, "finger prints," or other methods that allow for highly-detailed profiles of children. To the extent data brokers collect information from or about children, it should be used only to safeguard the child, such as prevention of fraud and identity theft.
- 3) If a data broker knows or reasonably should know it is collecting information from a teen, it should stop collecting, until and unless it has the teen's affirmative express and informed consent.

Big data can label and limit youth in ways that are not fully understood. Data brokers should allow children and teens the freedom to grow up unencumbered of such labels and limits.

3. Student Data

The baseline CPBR principles should also apply in the schoolhouse, where the rules governing privacy are woefully outdated. The White House Big Data Report rightly calls for an update to the Family Educational Rights and Privacy Act of 1974 (FERPA). We support modernizing FERPA (although specific recommendations for that sector-specific statute are beyond the scope of this submission). What is important here is that context matters. Therefore, it bears repeating Common Sense Media's three basic principles that attempt to balance the tremendous opportunity provided by education technology with the need to foster a trusted learning environment, where students' personal information is protected:

- 1) Students' personal information should be used solely for educational purposes;
- 2) Students' personal information or online activity should not be used to target advertising to students or families; and

⁴² The FTC Data Broker Report recommended legislation requiring that consumer-facing sources obtain affirmative express consent before they collect sensitive information, "such as certain health information." *Cf.* FTC Data Broker Report, *supra* note 11, at 52. Relatedly, Chairwoman Edith Ramirez and Commissioner Julie Brill also recommended that data brokers should take reasonable steps to assure themselves that their sources obtained data with notice and choice, "including express affirmative consent for sensitive data." *Id.* at 52 n.91. And Commissioner Brill separately supported "[a] requirement that the sources of data broker information used for marketing purposes provide consumer control over collection—express affirmative consent for sensitive information collection, notice and choice for other information..." Statement of Commissioner Julie Brill, *Data Brokers: A Call for Transparency and Accountability* C-4 (May 27, 2014).

- 3) Schools and education technology providers should adopt appropriate data security, retention, and destruction policies.

III. Conclusion

Big Data will shape our lives in ways both large and small. It will bring with it numerous benefits and efficiencies. But it should not be used to label or limit kids. Strong privacy legislation that takes into account the unique sensitivities of child, teen, and student data is urgently needed.

We thank the National Telecommunications and Information Administration for considering the implications of big data on the Consumer Privacy Bill of Rights and privacy legislation. We look forward to working with the Administration and other policymakers and stakeholders to ensure that kids, teens, and students can reap the benefits of big data while also staying safe from its risks.

Respectfully submitted,

A handwritten signature in black ink that reads "Jim Steyer". The signature is written in a cursive, flowing style.

James P. Steyer
CEO and Founder
Common Sense Media

APPENDIX A



March 31, 2014

Nicole Wong, Deputy Chief Technology Officer
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20502

ATTN: **Big Data Study – Comments of Common Sense Media**

Dear Ms. Wong,

Common Sense Media, a nonpartisan, nonprofit organization dedicated to helping kids, families, and educators thrive in a world of media and technology, respectfully submits these comments in response to the Office of Science and Technology Policy's Request for Information in the comprehensive review of issues at the intersection of "big data" and privacy. As the White House frames the key questions that the collection, analysis and use of "big data" raise for our government and nation, **we urge special consideration for the privacy interests of children and teens in both the consumer and education sectors. Today's youth are prolific users of the Internet and uniquely at risk when it comes to "big data."**

I. Introduction and Overview

Today's kids are the first generation to live their entire lives online, creating a vast digital footprint that can track them throughout their lives. The explosive growth of digital devices, smart phones, and social media is literally transforming the lives of these "digital natives" at home, at school, and in between. Even the youngest of our children are migrating online, using smart phones and tablets, downloading apps and content. These new high-tech tools bring a wonderful potential for our children to learn, communicate, and create – as well as the potential to amass a huge collection of personally identifiable information about young people that can be tracked, mined, and exploited by unintended audiences with surprising consequences.

The clear trends for young people to share more information online, to use more mobile technology, and for more technology to be integrated in schools, underscore the need for special protections for children, teens, and students. When it comes to big data and young people, we must ensure that their sensitive personal information is safeguarded, so they can enjoy innovative and engaging content and applications without surrendering their privacy.

Common Sense Media calls for measures to bolster existing protections for children and to empower teens with better choice and control over their online information. Specifically, all young users should be able to use an "Eraser Button" to delete information they post online. Teens should be able to "opt in" to online collection of their personal and geolocation information, and to "opt in" before their personal information, location, and online activity is shared with third parties for uses such as profiling or behavioral marketing.

Common Sense Media also calls for special protections for students, to help ensure that: students' sensitive personal information is used only for educational purposes; students' sensitive personal information and online activity is not used to target advertising to students or families; and appropriate data security, retention, and destruction policies are adopted for students' data.

We want to create a trusted environment where kids can use technology at home, at school, and on the go; where they can harness the power of the Internet for learning, entertainment, communication and collaboration; and where they can find their voice, share with their friends, and explore the world without fear of commercial exploitation or other unintended consequences.

II. Technological Trends Involving Children, Teens, and Students

A. Today's children and teens are heavy tech users, increasingly sharing personal information online.

Our children and teens are growing up in a digital world, surrounded by online and mobile technology. They have unprecedented access to digital products, create and consume enormous amounts of content, and can connect with people and information around the world. While the Internet presents tremendous opportunities for entertainment, innovation, and learning, this digital interaction also raises concerns about kids' and teens' online privacy and the creation of a huge digital footprint.

1. Young people are prolific online users.

Almost a quarter of children begin their digital lives before they are even born and, by the age of two, 92 percent of American children have an online presence.¹ By age five, about half of children go online daily. And, by age eight, more than two-thirds of children use the Internet on any given weekday.²

Teens are especially avid daily users of digital technology and social media. Virtually all teenagers (95 percent) use the Internet.³ Moreover, our kids live in a culture of sharing. Social media has become part of everyday life for many teens and a key communication tool. Our recent survey of teens found that 90 percent of 13- to 17-year-olds have used some form of social media, and 75 percent of teenagers have a profile on a social networking site.⁴

¹ Business Wire Press Release, *Digital Birth: Welcome to the Online World – AVG Study Finds a Quarter of Children Have Online Births Before Their Actual Birth Dates* (Oct. 6, 2010), <http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World>

² The Joan Ganz Cooney Center at Sesame Workshop, *Always Connected: The New Digital Media Habits of Young Children*, at 16 (Mar. 10, 2011), http://www.joanganzcooneycenter.org/wp-content/uploads/2011/03/jgcc_alwaysconnected.pdf.

³ Pew Research Center & Berkman Center for Internet and Society, *Teens and Technology 2013*, at 3 (Mar. 13, 2013), http://www.pewinternet.org/~media/Files/Reports/2013/PIP_TeensandTechnology2013.pdf.

⁴ Common Sense Media, *Social Media, Social Life: How Teens View Their Digital Lives* at 9 (Summer 2012), <http://www.common Sense Media.org/sites/default/files/research/socialmediasociallife-final-061812.pdf>

Notably, teens are increasingly sharing personal information on social media sites:

- 92 percent posted their real name to the profile they use most often;
- 91 percent posted a photo of themselves;
- 84 percent post their interests, such as movies, music or books they like;
- 82 percent post their birth date; and
- 71 percent post their school name and the city or town where they live.⁵

2. Young people are uniquely at risk online.

As children and teens surf the Internet, a host of cookies and other technologies tracks their movements and builds a profile of their online activities. Significantly, these youth have been tracked and targeted more than adults in online spheres. A 2010 *Wall Street Journal* investigation found that the top 50 websites popular with U.S. children and teens installed 30 percent more tracking technology on personal computers than top websites aimed at adults.⁶

When it comes to social media, although teens frequently share their personal details, some teens may not understand whether and how the information they share is being used by the social media site and by third parties. For instance, recent focus groups suggest that teen Facebook users did not believe that the company would give anyone else access to the information they share.⁷

Other research shows that even when Facebook users think they are using privacy controls to limit the information they are sharing “publicly,” they are increasingly revealing information “privately” and fail to appreciate that such “private” disclosures are available to Facebook, third-party apps, and Facebook advertisers.⁸

Moreover, whatever users text or post can be searched, copied, shared, and analyzed by vast social networks of friends and followers – and by vast commercial networks of advertisers, analytics services, and data brokers. This information can be used in unintended ways. According to a 2013 Kaplan survey, for example, 30 percent of college admissions officers discovered something on social media that negatively impacted the applicant’s chance of getting into the school.⁹ In addition, some lending companies are mining social media to determine creditworthiness and make lending decisions.¹⁰ Conceivably, a social media post about a youthful indiscretion could come back to haunt a young borrower.

⁵ Pew Research Center & Berkman Center for Internet & Society, *Teens, Social Media, and Privacy*, at 3 (May 21, 2013), http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

⁶ Steve Stecklow, *On the Web, Children Face Intensive Tracking*, WALL ST. J. (Sept. 17, 2010).

⁷ *Teens, Social Media, and Privacy*, supra note 5, at 10.

⁸ Stutzman, Gross & Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, J. PRIVACY & CONFIDENTIALITY, Vol. 4: Iss. 2, Article 2 (2013), <http://repository.cmu.edu/jpc/vol4/iss2/2>.

⁹ Press Release, *Kaplan Test Prep Survey: More College Admissions Officers Checking Applicants’ Digital Trails, But Most Students Unconcerned* (Oct. 31, 2013), <http://press.kaptest.com/press-releases/kaplan-test-prep-survey-more-college-admissions-officers-checking-applicants-digital-trails-but-most-students-unconcerned>

¹⁰ Stephanie Armour, *Borrowers Hit Social-Media Hurdles*, WALL ST. J. (Jan. 8, 2014).

B. The growth in mobile technology is especially significant for kids and teens.

The clear trend in recent years has been the huge shift to mobile technology. Not necessarily as evident is how quickly children are starting to use mobile devices at very young ages, how heavily teens have come to rely on mobile devices for Internet access, and how pervasively kids' apps have tracked young users.

1. Young children and teens are early adopters of mobile devices.

Common Sense Media's recent Research Report, *Zero to Eight, Children's Media Use in 2013*, found that almost twice as many young children are using mobile media now as there were just two years ago, and the average amount of time children spend using mobile devices has tripled. Seventy-two percent of children 0 to 8 have used a mobile device for some type of media activity, such as playing games, watching videos, or using apps. In fact, 38 percent of toddlers *under age two* have used a mobile device in the past year.¹¹

Teens especially are increasingly connected whenever and wherever they go – more so than adults:

- About three in four (74 percent) teens ages 12-17 say they access the Internet on cell phones, tablets, and other mobile devices at least occasionally;
- One in four teens are “cell-mostly” Internet users — far more than the 15 percent of adults who are cell-mostly;
- Among teen smartphone owners, half are cell-mostly Internet users.¹²

2. Mobile technology presents special risks, particularly for young users.

The explosive growth of mobile technology poses particular challenges because these devices can be used almost anytime, anywhere, providing a ready platform for users to share a nearly constant stream of personal information. The proliferation of apps can access a tremendous amount of personal data and usage information from mobile devices – including their precise geolocation. This sensitive personal information can be shared with advertisers, analytics companies, data brokers and other third parties, often without the user's knowledge or express consent. Even with privacy policies and on-screen permissions, it's not always easy for users to determine what information an app will access, how it will be used, or with whom it will be shared.

Research has shown that mobile apps for kids have been rampant leakers of personal information. A December 2012 Federal Trade Commission Report found that many of the kids' apps shared sensitive information with third parties -- without disclosing that fact to parents. Nearly 60 percent (235) of the apps reviewed transmitted device ID to the developer or, more commonly, an advertising network, analytics company, or other third party. Three percent

¹¹ Common Sense Media, *Zero to Eight: Children's Media Use in America 2013*, at 11 (Oct. 28, 2013), <https://www.commonsensemedia.org/file/zero-to-eight-2013pdf-0/download>.

¹² Pew Research Center & Berkman Center for Internet and Society, *Teens and Technology 2013* (Mar. 13, 2013), at http://www.pewinternet.org/~media/Files/Reports/2013/PIP_TeensandTechnology2013.pdf

(12) of the apps also transmitted the user's geolocation and one percent (3) transmitted the device's phone number. This is concerning because in every instance where an app transmitted geolocation or phone number, it also transmitted the user's device ID, so that third parties could potentially connect the location and phone information with any data previously collected through other apps running on the same device. These apps have been downloaded hundreds of thousands of times.¹³

Similarly, a June 2013 *Wall Street Journal* examination of 40 popular and free child-friendly apps on Google's Android and Apple's iOS systems found that nearly half transmitted to other companies a device ID number, a primary tool for tracking users from app to app, and 70 percent transmitted information about how the app was used.¹⁴

Although some tracking of young children may be curbed by recent amendments to the COPPA regulations, noted below, the opportunity for tracking, profiling, use and abuse of young people's sensitive information is vast.

C. Increasing use of technology in schools is spawning a proliferation of digital student data.

Our nation's schools are increasingly integrating computers, laptops and tablets in the classroom, and relying on cloud computing services for a variety of academic and administrative functions. This technology, used wisely, has the vast potential to enhance and personalize student learning and to improve school efficiency. To fulfill this potential, we must ensure that students' sensitive personal information is safeguarded.

Through online platforms, mobile applications, digital courseware, virtual forums for interacting with other students and teachers, and cloud computing services, schools and education technology providers collect massive amounts of sensitive information about students. This student data includes: school work and academic performance data, online searches, contact information, health information, behavior and disciplinary records, eligibility for free or reduced-price meals – even cafeteria selections and whether or not students ride the bus to school. This information is at risk.

Some online services collect and analyze personal details about students without clear limits on use of the student data for educational purposes.¹⁵ Other online services have failed to adequately secure and encrypt students' personal information from potential misuse.¹⁶ In fact, a recent study by Fordham Law School's Center on Law and Information Policy found that the majority of school district cloud service agreements have serious deficiencies in the protection of student information, "generally do not provide for data security and even allow vendors with

¹³ FTC, *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, at 10-11 (Dec. 2012).

¹⁴ Jeremy Singer-Vine and Anton Troianovski, *How Kid Apps Are Data Magnets*, WALL ST. J. (June 27, 2013).

¹⁵ See, e.g., Benjamin Herold, *Google Under Fire for Data-Mining Student Email Messages*, Education Week (Mar. 13, 2014), <http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html?cmp=ENL-EU-NEWS2>.

¹⁶ Natasha Singer, *Data Security Is A Classroom Worry, Too*, New York Times (June 22, 2013).

alarming frequency to retain student information in perpetuity.”¹⁷

Concerns about the privacy and security of this sensitive student information, if not addressed up front, can quash innovation in the education sector. Students shouldn’t have to surrender their right to privacy and security at the schoolhouse door. We need clear rules of the road to ensure that schoolchildren’s information is not exploited for commercial purposes and stays out of the wrong hands.

III. The Administration Should Ensure That Personal Data of Children, Teens, and Students Is Protected.

As the Administration considers the implications of “big data,” we urge that data collected from and about children, teens, and students be given special consideration and heightened protection. All data should not be considered equal. As the Administration recognized in its 2012 Consumer Privacy Bill of Rights, personal data obtained from children and teenagers may require greater protections than data for adults.¹⁸ Indeed, personal information about children and teens is a sensitive data category, like financial and health information, that warrants special protection. Likewise, the Federal Trade Commission’s 2012 Privacy Report recognized the general consensus that children’s information is a sensitive data category (like financial and health information, and precise geolocation data), and that companies should obtain affirmative express consent from consumers before collecting such data. The FTC further recognized that information about teens is sensitive, warranting consideration of additional protections, as well.¹⁹

With this in mind, we encourage the Administration to support the following measures:

A. Online protections for minors and the “Eraser Button.”

The Children’s Online Privacy Protection Act (“COPPA”), enacted in 1998, requires sites, services and apps that are directed to children under 13 or have actual knowledge that the user is under 13 to obtain parental consent before collecting personal information. The FTC recently updated its COPPA Rule to expand the type of personal information that requires parental consent to include geolocation, photos, videos, audio, and persistent identifiers, to account for the explosive growth of social media and mobile technologies.²⁰

¹⁷ Press Release, *Fordham Law National Study Finds Public School Use of Cloud Computing Services Causes Data Privacy Problems* (Dec. 13, 2013), <http://law.fordham.edu/32158.htm>; Natasha Singer, *Schools Use Web Tools, and Data is Seen at Risk*, New York Times (Dec. 12, 2013).

¹⁸ *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 15 (Feb. 2012).

¹⁹ FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 59-60 (Mar. 2012).

²⁰ See News Release, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children’s Online Privacy Protection Rule (Dec. 19, 2012), <http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over>.

To enhance control of online information for both children and teens, Common Sense Media has supported requiring Internet companies to provide an “Eraser Button” that would permit minors to remove content or information that they personally posted on websites, online services, and online or mobile apps. Too often, young people post information they later regret but can’t delete from the online and mobile world. Children and teens often self-reveal before they self-reflect and may post sensitive personal information about themselves -- and about others -- without realizing such sharing may affect potential college or job opportunities -- or even increase the risk of identity theft. All of us -- especially kids -- should be able to delete what we post.

According to a recent Pew poll, pruning and revising social media profile content is an important part of teens’ online identity management: 59 percent have deleted or edited something that they posted in the past. Moreover, 19 percent of teens have posted updates, comments, photos, or videos that they later regretted sharing.²¹

In September, 2013, California enacted SB 568, *Privacy Rights for California Minors*. This new “Eraser Button” law requires websites and apps to permit users under 18 to remove content they posted on Internet and social media sites.²² Several additional states are now considering similar measures. The FTC also has supported the “eraser button” concept, noting that it is consistent with the principles of data access and deletion.²³

Many companies already provide deletion functions for their users. Although not a panacea for information that has already been re-posted or shared by third parties, an eraser button would provide needed control for online profiles.

B. Additional online protections for teens and an “opt in” standard for collection and use of their sensitive information.

While many current online protections are geared to young children, teenagers also should be accorded special protections online. Teens are heavy users of the Internet and mobile technology, tech-savvy in some ways, yet still requiring training wheels in others. As the FTC has explained, more privacy-protective default settings for teens “can function as an effective ‘speed bump’ for this audience and, at the same time, provide an opportunity to better educate teens about the consequences of sharing personal information.”²⁴

Too many online and mobile companies launch services and access users’ information automatically, sometimes giving them the opportunity to opt out afterwards. This can mean that a user’s personal information is collected and used before the user understands how the service works. Especially when teens are targeted and sensitive information is involved, they should be

²¹ *Teens, Social Media, and Privacy*, supra note 5, at 9.

²² Press Release, *Governor Signs Steinberg Bill Protecting Minors’ Privacy on the Internet* (Sept. 23, 2013), <http://sd06.senate.ca.gov/news/2013-09-23-governor-signs-steinberg-bill-protecting-minors-privacy-internet>

²³ FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 70 (March 2012).

²⁴ *Id.* at 60.

given the opportunity to opt in.

We recognize that as teens mature it may not always be effective or appropriate to seek parental consent for their online conduct. That said, teens deserve enhanced online protection that would provide them with more transparency, notice, choice and control in the collection and use of their personal information.

Accordingly, Common Sense Media supports measures to require:

- “Opt In” for Collection of Personal Information: Online companies should obtain the teen’s express affirmative consent before collecting personal or location information;
- “Opt In” for Behavioral Marketing: Online companies should obtain the teen’s express affirmative consent before sharing personal information, location, or online activity for third-party profiling or behavioral marketing; and
- Fair information practice principles: Online companies should establish policies for transparency, collection, use, disclosure, retention, and security of teens’ personal information.

These protections are included in the bipartisan, bicameral Do Not Track Kids Act of 2013, which would provide important baseline protections for young teens.²⁵ The bill would amend COPPA to bolster protection for children under 13 and create new online and mobile privacy protections for teens who use websites/services directed to teens aged 13 to 15 (or that *know* they are collecting personal info from teens 13 to 15). The bill also includes a “Digital Marketing Bill of Rights for Teens” that establishes fair information practice principles and would require online companies to explain the types of personal information collected, how that information is used and disclosed, and the policies for collection of personal information.

As the Administration works with Congress to pass legislation that codifies the Consumer Privacy Bill of Rights into law, we respectfully urge the inclusion of similar measures to provided enhanced protection for teens.

The public overwhelmingly supports such proposals to rein in corporate surveillance, according to a survey recently conducted by Anzalone Liszt Grove Research. Online tracking of children and teens is especially concerning, with 89 percent of Americans stating that it is extremely or very important to keep personal information about our kids private from corporate tracking. In addition, the vast majority (78 percent) support requiring companies to get permission from young teens aged 13 to 15 before collecting any personal information about them or sending them targeted ads based on their online activities.²⁶

²⁵ S. 1700 and H.R. 3481, introduced in November, 2013, by Senator Edward J. Markey and Rep. Joe Barton.

²⁶ Memo from Anzalone Liszt Grover Research, Americans Concerned about Privacy from Corporate and Government Surveillance (Mar. 31, 2014), http://media.wix.com/ugd/c4876a_e8f4ee3b207344d9aac9a3403118ca9c.pdf.

C. Special privacy and data security protections for students.

It has long been recognized that student data deserves protection. New cloud computing technologies and the proliferation of student data in digital form heighten concerns that existing regulatory frameworks are inadequate. The Family Educational Rights and Privacy Act of 1974 (FERPA),²⁷ designed in the era of primarily paper records, gives parents the right to access their children's education records and generally requires written permission from the parent before these records are released to third parties. FERPA, however, is extremely complex and there are many significant gaps in coverage. Other statutes, such as the Protection of Pupil Rights Amendment (PPRA) and COPPA, also fail to cover large swaths of sensitive student data.

To pave the way for new personalized digital learning tools, online assessments, and other interactive technologies that help foster and enhance the learning process, the privacy and security of students' personal data must be addressed.

As Secretary of Education Arne Duncan stated, "Put plainly, student data must be secure, and treated as precious, no matter where it's stored. It is not a commodity."²⁸

Common Sense Media has proposed three basic principles that attempt to balance the tremendous opportunity provided by education technology with the need to foster a trusted learning environment, where students' personal information is protected:

1. Students' personal information should be used solely for educational purposes;
2. Students' personal information or online activity should not be used to target advertising to students or families; and
3. Schools and education technology providers should adopt appropriate data security, retention, and destruction policies.

There is overwhelming public support for the implementation of such policies and regulations to protect students' private information. A national survey conducted earlier this year on behalf of Common Sense Media found that 90 percent of adults – whether parents or not – are concerned about how non-educational interests are able to access and use students' personal information. Eighty-six percent of Americans agree that protecting children's safety and personal information should be the No. 1 priority, while only 11 percent believe the argument that regulations would be overly burdensome and stifle innovation.²⁹

²⁷ 20 U.S.C. § 1232g; 34 C.F.R. Part 99. The Protection of Pupil Rights Amendment (PPRA) also provides parents with the opportunity to opt-out of certain surveys and activities in schools when personal information is collected from the student for marketing purposes. PPRA, however, permits school districts to use personal information that they collect from students to develop, evaluate or provide educational products or services for students or schools. 20 U.S.C. § 1232h; 34 CFR Part 98.

²⁸ U.S. Dept. of Education, *Technology in Education: Privacy and Progress - Remarks of U.S. Secretary of Education Arne Duncan at the Common Sense Media School Privacy Zone Conference* (Feb. 24, 2014), <https://www.ed.gov/news/speeches/technology-education-privacy-and-progress>

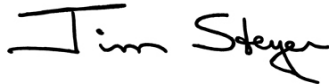
²⁹ Press Release, *National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared: Americans Overwhelmingly Support*

IV. Conclusion

The extraordinary technological changes and the development of new social, mobile, and educational platforms in recent years have created new and immersive environments for young people, resulting in a proliferation of sensitive digital data about them. We applaud the Administration for reviewing the implications of big data – and urge special attention to children, teens, and students in this review process and the development of public policy.

We look forward to working with the Administration as it continues this study, so we can fashion appropriate measures to safeguard the privacy and security of our children's personal data, and help ensure that the Internet remains a robust platform for education, innovation, and economic growth.

Respectfully submitted,

A handwritten signature in black ink that reads "Jim Steyer". The signature is written in a cursive, flowing style.

James P. Steyer
CEO and Founder
Common Sense Media

Reforms to Protect Students, Including Increased Transparency, Tighter Security Standards, and More Restrictions on Companies and Cloud Services (Jan. 22, 2014), at <http://www.common sense media.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern>.